JOURNAL OF NUMBER THEORY 46, 323–333 (1994)

Equidistant Arithmetic Codes and Character Sums*

DANIEL M. GORDON†

Department of Computer Science, University of Georgia, Athens, Georgia 30602

Communicated by R. L. Graham

Received March 22, 1991; revised June 11, 1992

A *cyclic arithmetic code* is a subgroup of $\mathbf{Z}/(r^n-1)\mathbf{Z}$, where the weight of a word x is the minimal number of nonzero coefficients in the representation $x \equiv \sum_{i=0}^{n-1} c_i r^i$ with $|c_i| < r$ for all i. A code is called *equidistant* if all nonzero codewords have the same weight. In this paper necessary conditions for the existence of equidistant codes are given. By relating these conditions to character sums on certain intervals, it is shown that for $r = 2, 3$ no new equidistant codes exist, and several infinite families of equidistant codes are given. © 1994 Academic Press, Inc.

1. INTRODUCTION

Arithmetic codes are designed to correct errors in computer arithmetic, rather than errors in transmission of bits handled by standard error-correcting codes. Arithmetic is done in $\mathbf{Z}/m\mathbf{Z}$, where $m = r^n \pm 1$, where r is the radix of the machine. This choice of modulus is convenient for arithmetic operations (see [10]).

In this context, an error consists of changing a digit, i.e., adding cr^j for some $|c| < r$ and $0 \leqslant j < n$. The distance $d(x, y)$ is the minimal number of errors needed to transform x into $y \pmod m$. The weight of an integer x is $d(x, 0)$.

We will write out any representation $x \equiv \sum_{i=0}^{n-1} c_i r^i \pmod m$ as $(c_{n-1}, c_{n-2}, \ldots, c_0)$. One way to find the weight of x is to find the minimal weight representation of x. For $m = r^n - 1$, this representation is unique (with a few exceptions), and is called the *cyclic nonadjacent form* (CNAF) of x. A cyclic shift of a CNAF is also a CNAF. The CNAF of rx is $(c_{n-2}, c_{n-3}, \ldots, c_0, c_{n-1})$. For more information on CNAFs, including an algorithm to construct them, see van Lint [12].

* This work was performed while the author was at Sandia National Laboratories, under U.S. Department of Energy Contract DE-AC04-76DP000789.

† Present address: Center for Communications Research, 4320 Westerra Court, San Diego, CA 92121. E-mail address: gordon@ccrwest.org.

0022-314X/94 $6.00

Let $AB = m$, with $m = r^n - 1$. A cyclic arithmetic code is a subgroup $C = \{AN \mid 0 \leqslant N < B\}$ of $\mathbf{Z}/m\mathbf{Z}$. We will be interested in the case where $B = p$ is a prime. Such a code will be denoted $C(p, r)$. We may assume that $n = \mathrm{ord}_p(r)$, the order of r modulo p, since otherwise $C(p, r)$ is a repetition of the code of length $\mathrm{ord}_p(r)$. It will be easier to study $\mathbf{Z}/m\mathbf{Z}/C \cong \mathbf{F}_p$.

Let $\langle r \rangle$ be the subgroup of $\mathbf{F}_p^*$ generated by r. Then we have [12, Theorem 10.2.10]:

PROPOSITION 1. *The weight of x is equal to the number of elements y of the coset $\langle r \rangle x$ for which*

$$\left\lfloor \frac{p}{r+1} \right\rfloor < y \leqslant \left\lfloor \frac{rp}{r+1} \right\rfloor.$$

An arithmetic code is called *equidistant* if all of its nonzero codewords have the same weight. Clark and Liang in [4] investigated equidistant codes for $r = 2$, and in [3] Clark and Lewis studied codes with general radix.

For any codeword x, the entire coset $\langle -1, r \rangle x$ is also in the code. Each element of the coset has the same weight, since the CNAF of $r^j x$ is a cyclic shift of the CNAF of x, and the CNAF of $-x$ is the negation of the CNAF of x.

Thus $\mathbf{F}_p^*$ may be partitioned into cosets of $\langle -1, r \rangle$, with each coset having the same weight.

Let d be the number of these cosets, i.e., the index of $\langle -1, r \rangle$ in $\mathbf{F}_p^*$ (in [3, 4], d is the index of $\langle r \rangle$ in $\mathbf{F}_p^*$, which is either equal to or twice our d). An obvious condition for C to be equidistant is if $d = 1$, which happens when r or $-r$ is a primitive root modulo p. In this case there is only one coset, and so all codewords have the same weight. These are the Mandlebaum–Barrows codes.

For $d > 1$ there are several cosets, which must have equal weight for the resulting code to be equidistant. No such codes exist for $r = 2$ or $r = 3$, as will be shown in Section 4, but computer searches for $4 \leqslant r \leqslant 5000$ and $p \leqslant 40{,}000$, as well as $r \leqslant 30$ and $p \leqslant 10^6$, reveal many such codes, with $d = 2, 3, \ldots, 10$. Presumably further searches would reveal larger values of d.

2. EQUIDISTANT CODES WITH $d = 2$

Equidistant codes with $d = 2$ are far more common than larger values of d. The radices $r = 5$ and $r = 11$ have more equidistant codes than other radices, which is explained by the following theorems:

THEOREM 1. *If* $r = 5$, $p \equiv 5 \pmod 8$, *and* $|\langle -1, 5\rangle| = (p-1)/2$, *then* $C(p, 5)$ *is equidistant.*

Proof. $d = 2$, so there are two cosets. The coset $\langle -1, 5\rangle$ consists of the quadratic residues, and the coset $2\langle -1, 5\rangle$ consists of the quadratic nonresidues. Since -1 is a residue, the residues and nonresidues are symmetric about $(p-1)/2$. By Proposition 1, the cosets will have equal weight if and only if the number of residues and nonresidues in $[\lfloor p/6\rfloor + 1, \ldots, \lfloor 5p/6\rfloor]$ are equal. This is true if and only if the number of residues and nonresidues in $[1, \lfloor p/6\rfloor]$ are equal, i.e.,

$$\sum_{i=0}^{\lfloor p/6\rfloor} \left(\frac{i}{p}\right) = 0.$$

This result was shown by Berndt, in Corollary 6.2 of [2]. ∎

THEOREM 2. *If* $r = 11$, $p \equiv 5 \pmod 8$, $p \equiv 2 \pmod 3$, *and* $|\langle -1, 11\rangle| = (p-1)/2$, *then* $C(p, 11)$ *is equidistant.*

Proof. This proof is the same as for the previous theorem. In [2] it is also shown that for $p \equiv 5 \pmod 8$ and $p \equiv 2 \pmod 3$,

$$\sum_{i=0}^{\lfloor p/12\rfloor} \left(\frac{i}{p}\right) = 0. \quad \blacksquare$$

A slightly modified version of Artin's conjecture implies that there are infinitely many primes satisfying the conditions of Theorems 1 and 2. The conjecture follows from the Generalized Riemann Hypothesis, as shown by Hooley in [9]. Let $v_5(x)$ be the number of primes less than x satisfying the conditions of Theorem 1, and $v_{11}(x)$ be the number of primes less than x satisfying the conditions of Theorem 2. Let A denote Artin's constant:

$$A = \prod_{q \text{ prime}} \left(1 - \frac{1}{q(q-1)}\right).$$

Then it may be shown, assuming the Generalized Riemann Hypothesis, that

$$v_5(x) \sim \frac{9A}{38}\pi(x) \approx 0.0886\,\pi(x), \tag{1}$$

and

$$v_{11}(x) \sim \frac{81A}{545}\pi(x) \approx 0.0556\,\pi(x). \tag{2}$$

In general, equidistant codes with $d=2$ occur if and only if $|\langle -1, r\rangle| = (p-1)/2$, and $\sum_{i=0}^{\lfloor p/(r+1)\rfloor}(i/p)$ is zero. In [2] various cases are given where this sum is always zero, positive, or negative. Let $S_{ab}=\sum_{i=\lfloor (b-1)p/a\rfloor}^{\lfloor bp/a\rfloor}(i/p)$. Then the results quoted above are that S_{61} and $S_{12,1}$ are always zero for $p\equiv 5 \pmod 8$. S_{31} and S_{41} are always positive for $p\equiv 1 \pmod 4$, which implies that there are no equidistant codes with $d=2$ for $r=2$ or $r=3$.

Most other values of $S_{r+1,1}$ are equal to zero occasionally and unpredictably. These lead to equidistant codes for most values of r, but not families as regular as those of Theorems 1 and 2.

3. Equidistant Codes with $d>2$

For higher values of d, we need to look at higher-order characters. Let $\zeta_d=e^{2\pi i/d}$, and g be a primitive root modulo p. Let $\log_g x$ be the discrete log of x in $\mathbf{F}_p$. Then define a dth-power residue character modulo p by

$$\left(\frac{a}{p}\right)_d=\zeta_d^{\log_g a}. \tag{3}$$

For $d=2$ this character is the standard Legendre symbol $(a \mid p)$. For larger values of d we may generalize the earlier arguments.

In the following, let p be a prime, r an integer less than p, and $d=(p-1)/|\langle -1, r\rangle|>1$.

Lemma 1. *$(a \mid p)_d$ is constant on cosets of $\langle -1, r\rangle$, with different values on distinct cosets.*

Proof. Since $\langle -1, r\rangle$ has index d, it is just the set of dth powers, and so by (3) each member has $(a \mid p)_d=1$. If two elements a and b from different cosets have $(a \mid p)_d=(b \mid p)_d$, then $(a^{-1}b \mid p)_d=1$ implies $a^{-1}b\equiv \pm r^j \pmod p$ for some j, so $a\langle -1, r\rangle = b\langle -1, r\rangle$. ∎

Theorem 3. *$C(p, r)$ is equidistant if and only if*

$$\sum_{i=1}^{\lfloor p/(r+1)\rfloor}\left(\frac{i}{p}\right)_d^s=0 \qquad \text{for} \quad 1\leqslant s\leqslant d-1. \tag{4}$$

Proof. The weight of a number a is equal to the number of elements of $a\langle -1, r\rangle$ in the interval

$$\left\{\left\lfloor\frac{p}{r+1}\right\rfloor+1, \ldots, \left\lfloor\frac{rp}{r+1}\right\rfloor\right\}.$$

For an equidistant code, this number is the same for all a. Since $(-1 \mid p)_d=1$, the dth power residues are symmetric about $(p-1)/2$, and

so the number of elements of $a\langle -1, r\rangle$ in $\{1, ..., \lfloor p/(r+1)\rfloor\}$ is also equal for all a. By Lemma 1 this means that every root of unity is represented an equal number of times in the interval, and so (4) follows.

For the other direction, notice that for any integer a prime to p,

$$\sum_{s=1}^{d} \left(\frac{a}{p}\right)_d^{-s} \sum_{i=1}^{\lfloor p/(r+1)\rfloor} \left(\frac{i}{p}\right)_d^{s} = d \sum_{\substack{1 \leqslant i \leqslant \lfloor p/(r+1)\rfloor \\ i \in a\langle -1, r\rangle}} 1.$$

Thus if (4) holds, the above sum is equal to $\lfloor p/(r+1)\rfloor$, which shows that each coset of $\langle -1, r\rangle$ is represented by exactly $\lfloor p/(r+1)\rfloor/d$ elements in $\{1, ..., \lfloor p/(r+1)\rfloor\}$, and so $C(p, r)$ is equidistant. ∎

The necessary condition resulting from just taking $s=1$ in (4) is not sufficient. For example, for $d=4$, $r=5$, and $p=401$, and $g=3$, in the range $\{1, ..., 66\}$ there are 18 fourth powers, 18 numbers with $(a \mid 401)_4 = -1$, 15 with $(a \mid 401)_4 = i$, and 15 with $(a \mid 401) = -i$. Thus the sum is zero, but the cosets have different weight. For prime d, it is sufficient:

COROLLARY 1. *If* $\sum_{i=1}^{\lfloor p/(r+1)\rfloor} (i/p)_d = 0$, *and* d *is prime, then* $C(p, r)$ *is equidistant.*

Proof. Since d is prime, $x^{d-1} + \cdots + x + 1$ is irreducible, and so the only combination of values of $(a \mid p)_d$ (which are restricted to dth roots of unity) which can sum to zero are equal numbers of each root of unity. Thus if the sum is zero, by Lemma 1 each coset must occur an equal number of times, and so $C(p, r)$ is equidistant. ∎

Theorem 3 can be used to show that there are infinite number of equidistant codes for many $d > 2$:

COROLLARY 2. *For any* $d \geqslant 2$, *let* $p \equiv 1 \pmod d$ *be a prime with* $(-1 \mid p)_d = 1$. *Suppose* $\mathbf{F}_p^*/(\mathbf{F}_p^*)^d$ *has* $1, 2, ..., d$ *as a complete system of representatives. Then for any* r *with* $\lceil p/(d+1)\rceil < r+1 \leqslant \lfloor p/d\rfloor$ *and* $|\langle -1, r\rangle| = (p-1)/d$, $C(p, r)$ *is an equidistant arithmetic code.*

Proof. By our choice of r and p, $\langle -1, r\rangle = (\mathbf{F}_p^*)^d$ and $\lfloor p/(r+1)\rfloor = d$. Since $\{1, 2, ..., d\}$ form a complete system of representatives, we have

$$\sum_{i=1}^{\lfloor p/(r+1)\rfloor} \left(\frac{i}{p}\right)_d^{s} = 1 + \zeta_d^s + \zeta_d^{2s} + \cdots + \zeta_d^{(d-1)s} = 0$$

for $1 \leqslant s \leqslant d-1$, and so by Theorem 3, $C(p, r)$ is an equidistant code. ∎

If we can find p and r satisfying the conditions of Corollary 2, then $C(p, r)$ will be an equidistant arithmetic code with index d. Choose p so

that -1 is a dth power residue modulo p. By Theorem 3.11 of [13], the number of dth power residues in $(\lceil p(d+1)\rceil, \lfloor p/d \rfloor)$ is

$$\frac{p}{d(d+1)}\{1+O(p^{-5/24})\}.$$

From this it follows that the number of dth powers in the interval that are not kdth powers for any $k>1$ is

$$\varphi\left(\frac{p-1}{d}\right)\frac{1}{d(d+1)}\left\{1+O\left(p^{-5/24}\cdot\tau\left(\frac{p-1}{d}\right)\right)\right\}, \tag{5}$$

where $\tau(N)$ is the number of divisors of N. Since $\tau(N)<N^{\varepsilon}$ for any ε and N sufficiently large (see [8]), (5) is positive for sufficiently large p. Thus, for p large enough, there will be such an $r\in(\lceil p/(d+1)\rceil, \lfloor p/d \rfloor)$ with $|\langle -1, r\rangle| = (p-1)/d$.

It is not known for which d there are primes such that $\{1, 2, ..., d\}$ form a complete system of representatives for $\mathbf{F}_p^*/(\mathbf{F}_p^*)^d$. If such a prime exists for a given d, then the function $(i \mid p)_d$ defines a mapping f from $\{1, ..., d\}$ to the cyclic group of order d, where $f(xy)=f(x)+f(y)$ for $1\leqslant xy\leqslant d$. Forcade and Pollington call such a mapping is called a *logarithm* in [6]. They show that such a mapping exists for $d<195$, but does not exist for $d=195$. If $d+1$ or $2d+1$ is prime, then a logarithm exists for d.

If such a logarithm exists, then by the Čebotarev density theorem there are an infinite number of primes with $\{1, 2, ..., d\}$ in different classes modulo $(\mathbf{F}_p^*)^d$ (see [11] for details). Therefore we have:

THEOREM 4. *For all $d<195$, and all d such that $d+1$ or $2d+1$ is prime, there are an infinite number of primes p and integers r for which $C(p, r)$ is an equidistant arithmetic code with index d.*

4. NONEXISTENCE RESULTS

In [4] Clark and Liang conjecture that there are no prime cyclic arithmetic codes for $r=2$ with $d>1$. By Theorem 3, it suffices to show that (4) never holds.

For any character χ modulo k, let $G(n, \chi)$ denote the Gauss sum

$$G(n, \chi)=\sum_{j=1}^{k}\chi(j)\,e^{2\pi inj/k},$$

and let $G(\chi)=G(1, \chi)$. The following lemma, due to Berndt, is a special case of (4.1) in [1]:

LEMMA 2. *Let χ be a primitive and even character with modulus p. Then*

$$\sum_{a \leq k \leq b}{}' \chi(k) = \frac{2G(\chi)}{p} \sum_{n=1}^{\infty} \overline{\chi(n)} \int_a^b \cos\left(\frac{2\pi n x}{p}\right) dx,$$

where the prime on the summation sign indicates that if a or b is integral, then the associated summands must be halved.

THEOREM 5. *Let p be prime, $r = 2$, $(p-1)/|\langle -1, r\rangle| = d > 1$. Then*

$$\sum_{i=1}^{\lfloor p/3 \rfloor} \left(\frac{i}{p}\right)_d \neq 0.$$

Proof. By Lemma 2 we have

$$\begin{aligned}\sum_{i=1}^{\lfloor p/3 \rfloor} \left(\frac{i}{p}\right)_d &= \frac{2G((|p)_d)}{p} \sum_{n=1}^{\infty} \overline{\left(\frac{n}{p}\right)_d} \int_0^{p/3} \cos\left(\frac{2\pi n x}{p}\right) dx \\ &= \frac{G((|p)_d)}{\pi} \sum_{n=1}^{\infty} \overline{\left(\frac{n}{p}\right)_d} \frac{1}{n} \sin\left(\frac{2\pi n}{3}\right) \\ &= \frac{\sqrt{3}\, G((|p)_d)}{2\pi} \sum_{n=0}^{\infty} \left(\overline{\left(\frac{3n+1}{p}\right)_d} \frac{1}{3n+1} - \overline{\left(\frac{3n+2}{p}\right)_d} \frac{1}{3n+2}\right).\end{aligned}$$

Let $\chi_{3p}(n) = (n \mid 3)(n \mid p)_d$. Then the above sum becomes

$$\frac{\sqrt{3}\, G((|p)_d)}{2\pi} \sum_{n=0}^{\infty} \frac{\overline{\chi_{3p}}(n)}{n} = \frac{\sqrt{3}\, G((|p)_d)}{2\pi} L(1, \overline{\chi_{3p}}).$$

$|G((|p)_d)| = \sqrt{p}$, and $L(1, \chi)$ is nonzero for any nonprincipal character (this is due to Dirichlet; see [5] for a proof). This implies the theorem. ∎

COROLLARY 3. *For $r = 2$, no equidistant codes with $d > 1$ exist.*

By the same method, we can show that there are no equidistant codes with $d > 1$ for $r = 3$:

THEOREM 6. *Let p be prime, $r = 3$, $(p-1)/|\langle -1, r\rangle| = d > 1$. Then*

$$\sum_{i=1}^{\lfloor p/4 \rfloor} \left(\frac{i}{p}\right)_d \neq 0.$$

Proof. Let

$$\chi_4(n) = \begin{cases} (-1)^{(n-1)/2}, & n \text{ odd}, \\ 0, & n \text{ even}, \end{cases}$$

and $\chi_{4p}(n) = \chi_4(n)(n \mid p)_d$. Then

$$\begin{aligned}
\sum_{i=1}^{\lfloor p/4 \rfloor} \left(\frac{i}{p}\right)_d &= \frac{2G((\mid p)_d)}{p} \sum_{n=1}^{\infty} \overline{\left(\frac{n}{p}\right)_d} \int_0^{p/4} \cos\left(\frac{2\pi n x}{p}\right) dx \\
&= \frac{G((\mid p)_d)}{\pi} \sum_{n=1}^{\infty} \overline{\left(\frac{n}{p}\right)_d} \frac{1}{n} \sin\left(\frac{\pi n}{2}\right) \\
&= \frac{G((\mid p)_d)}{\pi} \sum_{n=0}^{\infty} \left(\overline{\left(\frac{4n+1}{p}\right)_d} \frac{1}{4n+1} - \overline{\left(\frac{4n+3}{p}\right)_d} \frac{1}{4n+3} \right) \\
&= \frac{G((\mid p)_d)}{\pi} \sum_{n=0}^{\infty} \frac{\overline{\chi_{4p}}(n)}{n} \\
&= \frac{G((\mid p)_d)}{\pi} L(1, \overline{\chi_{4p}}).
\end{aligned}$$

As before, this is never zero. ∎

COROLLARY 4. *For $r = 3$, no equidistant codes with $d > 1$ exist.*

One further result, due to W. Li, shows that Theorem 1 gives all equidistant codes for $r = 5$.

THEOREM 7. *Let χ be a nontrivial even character of $\mathbf{Z}$ modulo an odd prime $p > 3$. Let $\chi_{3p}(n) = (n \mid 3)\,\chi(n)$,*

$$\chi_6(n) = \begin{cases} (n \mid 3), & n \text{ odd}, \\ 0, & n \text{ even}, \end{cases}$$

and $\chi_{6p}(n) = \chi_6(n)\,\chi(n)$. Then

$$\sum_{i=1}^{\lfloor p/6 \rfloor} \chi(i) = \frac{\sqrt{3}\, G(\chi)}{2\pi} L(1, \overline{\chi_{6p}}) \frac{2 + 2\bar{\chi}(2)}{2 + \bar{\chi}(2)}.$$

Proof. By Lemma 2,

$$\begin{aligned}
\sum_{i=1}^{\lfloor p/6 \rfloor} \left(\frac{i}{p}\right)_d &= \frac{2G(\chi)}{p} \sum_{n=1}^{\infty} \overline{\left(\frac{n}{p}\right)_d} \int_0^{p/6} \cos\left(\frac{2\pi n x}{p}\right) dx \\
&= \frac{G(\chi)}{\pi} \sum_{n=1}^{\infty} \overline{\left(\frac{n}{p}\right)_d} \frac{1}{n} \sin\left(\frac{2\pi n}{6}\right) \\
&= \frac{\sqrt{3}\, G(\chi)}{2\pi} \sum_{n=0}^{\infty} \frac{\bar{\chi}(6n+1)}{6n+1} + \frac{\bar{\chi}(6n+2)}{6n+2} - \frac{\bar{\chi}(6n+4)}{6n+4} - \frac{\bar{\chi}(6n+5)}{6n+5} \\
&= \frac{\sqrt{3}\, G(\chi)}{2\pi} \left(L(1, \overline{\chi_{6p}}) + \frac{\bar{\chi}(2)}{2} L(1, \overline{\chi_{3p}}) \right). \qquad (6)
\end{aligned}$$

Since

$$L(1, \overline{\chi_{3p}}) = \frac{2}{2 - \overline{\chi_{3p}}(2)} \sum_{\substack{n \text{ odd} \\ n>0}} \frac{\overline{\chi_{3p}}(n)}{n} = \frac{2}{2 + \bar{\chi}(2)} L(1, \overline{\chi_{6p}}),$$

we get that (6) is equal to

$$\frac{\sqrt{3}\, G(\chi)}{2\pi} L(1, \overline{\chi_{6p}}) \left(1 + \frac{\bar{\chi}(2)}{2} \frac{2}{1 + \bar{\chi}(2)}\right) = \frac{\sqrt{3}\, G(\chi)}{2\pi} L(1, \overline{\chi_{6p}}) \frac{2 + 2\bar{\chi}(2)}{2 + \bar{\chi}(2)}. \quad \blacksquare$$

COROLLARY 5. *For $r = 5$, no equidistant codes with $d > 2$ exist. For $d = 2$, $C(p, 5)$ is an equidistant code if and only if $p \equiv 5 \pmod 8$ and $|\langle -1, 5 \rangle| = (p-1)/2$.*

Proof. By Theorem 3, $C(p, 5)$ is equidistant if and only if (6) is zero for $\chi = (\,|\,p)_d^s$, for $s = 1, \ldots, d-1$. Since $L(1, \overline{\chi_{6p}})$ is nonzero, this is equivalent to $(2\,|\,p)_d^s = -1$ for $s = 1, \ldots, d-1$. This is clearly impossible for $d > 2$. For $d = 2$, $(2\,|\,p)_d = -1$ implies that $p \equiv 3, 5 \pmod 8$. Since $|\langle -1, 5 \rangle| = (p-1)/2$, -1 is a quadratic residue, and we have $p \equiv 5 \pmod 8$. $\blacksquare$

One other case appears to be of special interest: computer searches show that for $r = 27$ there are no equidistant codes with $p < 10^6$. It is possible to apply Lemma 2 to this case, but the resulting expression does not seem to have a simple expression as a character sum.

By elementary methods, we can obtain a partial result:

THEOREM 8. *For $r = 27$ and $d = 2$, no equidistant codes exist.*

Proof. If $p \equiv 1 \pmod 3$, then -1 and 27 are cubes mod p, and so $|\langle -1, 27 \rangle| \leqslant (p-1)/3 < (p-1)/2$. If $p \equiv 2 \pmod 3$, then 27 and -1 cannot both be squares, since $(27\,|\,p) = (3\,|\,p) = (-1\,|\,p)(p\,|\,3) = -(-1\,|\,p)$. $\blacksquare$

The fact that no equidistant codes for $r = 27$ and $d > 2$ exist for $p < 10^6$ is not conclusive. If we pretend that $(i\,|\,p)_d$ is a random dth root of unity, then the probability that (4) holds is roughly

$$\frac{\binom{\lfloor p/(r+1) \rfloor}{\lfloor p/(d(r+1)) \rfloor, \lfloor p/(d(r+1)) \rfloor, \ldots, \lfloor p/(d(r+1)) \rfloor}}{{}_d\lfloor p/(d(r+1)) \rfloor} = O(p^{-(d-1)/2}),$$

where the implied constant depends on r.

Summing this over the primes less than x, we get that the expected number of equidistant codes for a fixed r and d is

$$\sum_{p<x} p^{-(d-1)/2} = \begin{cases} O(\sqrt{x}/\log x), & d=2 \\ O(\log\log x), & d=3 \\ O(1), & d>3. \end{cases}$$

This heuristic reasoning does not work for $r=2$, 3, 5, and 11, as shown in earlier theorems, but is consistent with results for most other values of r. It also suggests why equidistant codes with $d>2$ are so rare. It remains an open problem to prove that any r has an infinite number of equidistant codes with $d=3$, or that any $r>5$ has a finite number of equidistant codes with $d>3$.

ACKNOWLEDGMENTS

The author thanks W. Li, for pointing out that the original version of Theorem 3 could be strengthened, and that Theorem 7 followed from it. She also encouraged further efforts, which led to Theorem 4.

REFERENCES

1. B. C. BERNDT, Periodic Bernoulli numbers, summation formulas and applications, *in* "Theory and Application of Special Functions" (R. A. Askey, Ed.), pp. 143–189, Academic Press, New York, 1975.
2. B. C. BERNDT, Classical theorems on quadratic residues, *Enseign. Math.* (2) **22** (1976), 261–304.
3. W. E. CLARK AND L. W. LEWIS, Prime cyclic arithmetic codes and the distribution of power residues, *J. Number Theory* **32** (1989), 220–225.
4. W. E. CLARK AND J. J. LIANG, Equidistant binary arithmetic codes, *IEEE Trans. Inform. Theory* **32** (1986), 106–108.
5. H. DAVENPORT, "Multiplicative Number Theory," 2nd ed., Graduate Texts in Math., Vol. 74, Springer-Verlag, New York, 1980.
6. R. W. FORCADE AND A. D. POLLINGTON, What is special about 195? Groups, nth power maps and a problem of Graham, *in* "Proceedings of the First Conference of the Canadian Number Theory Association, Banff, 1988" (R. A. Mollin, Ed.), de Gruyter, Berlin, 1990.
7. D. M. GORDON, Perfect multiple error-correcting codes, *Math. Comp.* **49** (1987), 621–633.
8. G. H. HARDY AND E. M. WRIGHT, "An Introduction to the Theory of Numbers," 4th ed., Clarendon, Oxford, 1965.
9. C. HOOLEY, On Artin's conjecture, *J. Reine Angew. Math.* **225** (1967), 209–220.
10. D. E. KNUTH, "The Art of Computer Programming," 2nd ed., Vol. 2, Addison–Wesley, Reading, MA, 1981.

11. H. W. LENSTRA, Jr., Perfect arithmetic codes, *in* "Seminaire Delange–Pisot–Poitou, Théorie des Nombres, 1977–1978."
12. J. H. VAN LINT, "Introduction to Coding Theory," Graduate Texts in Math., Vol. 86, Springer-Verlag, New York, 1982.
13. K. K. NORTON, On the distribution of kth power residues and non-residues modulo n, *J. Number Theory* **1** (1969), 398–418.